pkIRISGrid

Una PKI para IRISGrid

- Requisitos pkIRISGrid 0.2 beta – EUGridPMA
  - Cumplidos – v3.2 - 02/02/2005
- Estructura Funcional
- Tecnología usada
- Operación de la PKI
  - Capturas de pantalla
- ¿Y ahora qué?

- Requisitos pkIRISGrid 0.2 beta – EUGridPMA
  - Cumplidos – v3.2 - 02/02/2005
- Estructura
- Tecnología usada
- Operación
  - Capturas de pantalla
- ¿Y ahora qué?

- Controles de seguridad en la CA
  - Máquina dedicada
  - Portatil sin tarjeta de Red
  - Descansa siempre en una caja fuerte ignífuga
  - Claves y certificados en llaves USB guardadas en la caja fuerte
- Espacio de nombres
  - dc=irisgrid, dc=es
    - cn=nombre@nombre, [o=nombre], dc=irisgrid, dc=es
    - cn=nombre.nombre, [o=nombre], dc=irisgrid, dc=es
- Políticas/Documentación
  - Política de Certificación (CP) y Prácticas de Certificación (CPS)
  - **1.3.6.1.4.1.7547**.2.1.4.X - Sucesivas versiones de IRISGrid-CA
  - **1.3.6.1.4.1.7547**.2.2.4.X.X - IRISGrid-CA CPS versión X.X

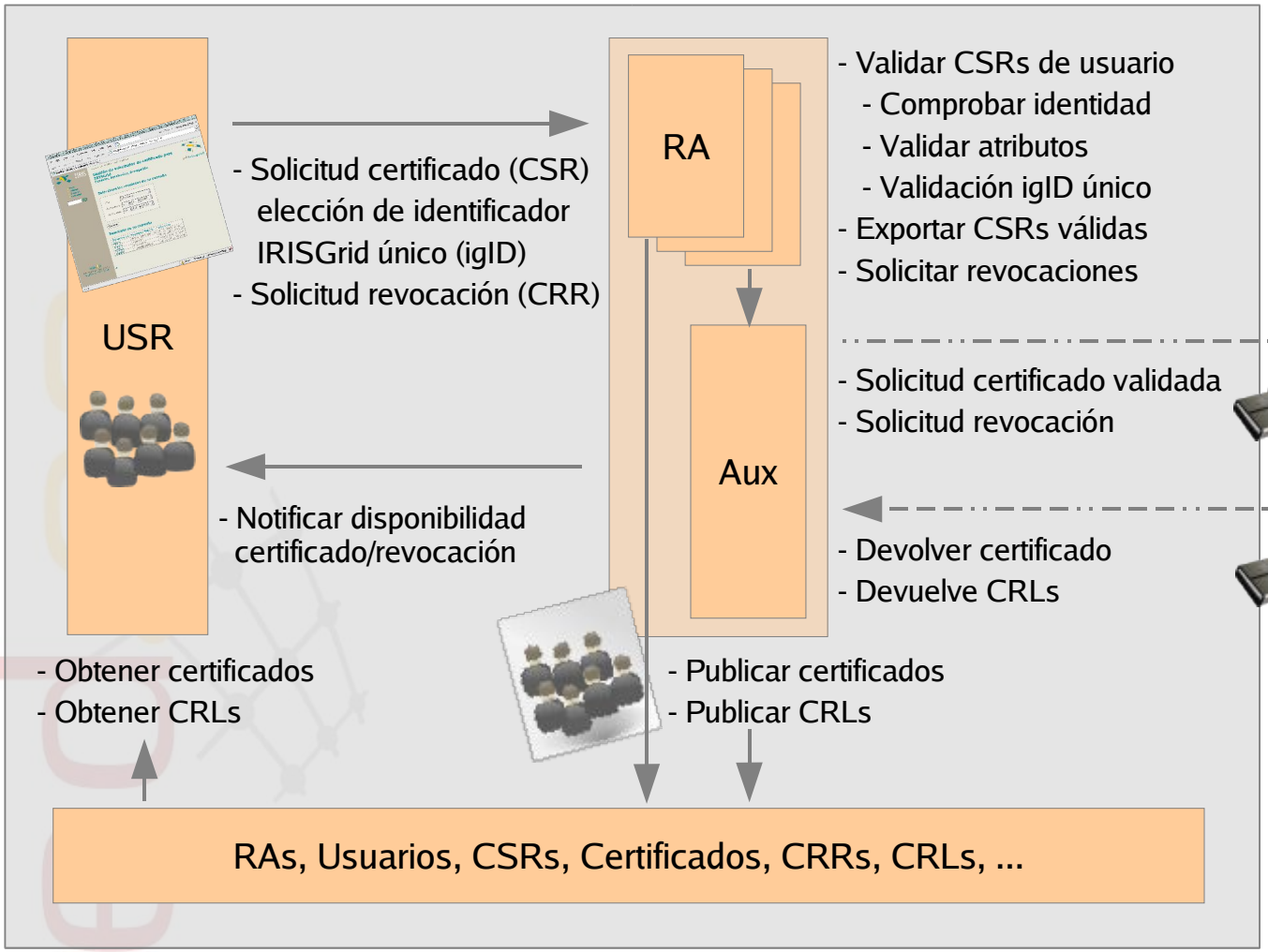
- Certificados
  - Expedirlos y revocarlos
  - Almacenar los certificados emitidos y las fechas de revocación de los mismos
  - Publicar información de revocación periódicamente
- Revocación
  - Solicitadas por usuario final, administrador RA y la propia CA
- Registro de eventos
  - Se guardan logs de todos los eventos necesarios
- Auditorías
  - La CA debe poder auditar a los gestores de las RAs al menos una vez al año

- RAs alojadas en RedIRIS (web)
  - Usuario - http://**ra1**.irisgrid.es
  - Administrador - http://**ra1**.irisgrid.es/**admin**/
- Identificación de entidades
  - Cada gestor/operador de RA debe conocer a sus usuarios
  - Validar identidades finales y atributos
- Unicidad en la asignación de nombres
  - No existe un sistema global de nombres que permita identificar a todo el mundo sin ambigüedad. ¿Qué tipo de nombre usamos?
  - DN: cn=j.masa@rediris.es, dc=irisgrid, dc=es
- Seguridad en la comunicación con la CA
  - Módulo auxiliar y llaves USB para intercambio de información

- Al estilo mail
- NO ES MAIL

- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura Funcional
- Tecnología usada
- Operación
  - Capturas de pantalla
- ¿Y ahora qué?

pkIRISGrid. Estructura funcional



- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- Tecnología usada
- Operación
  - Capturas de pantalla
- ¿Y ahora qué?

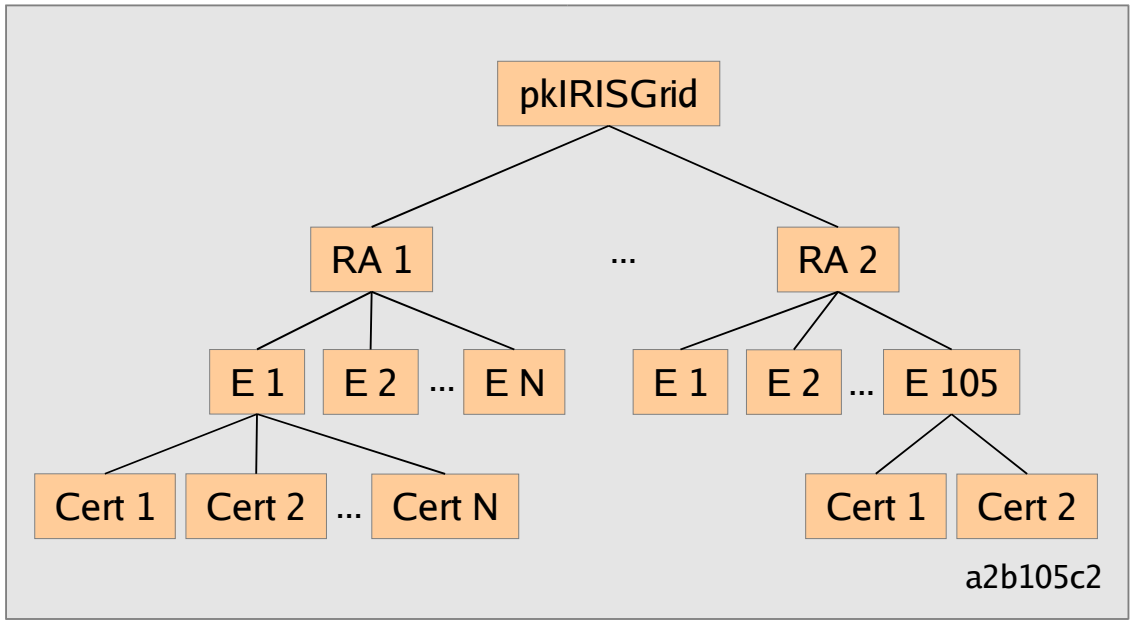
Tecnología usada en pkIRISGrid

- OpenSSL
- LDAP (esquema pkirisgrid)
  - Base de almacenamiento de RAs, Entidades (usuarios, servicios/servidores), CSRs, CRRs, certificados, CRLs
- COPA (Codificación optimizada para el acceso jerárquico a la información)
  - **a1b105c2** identifica a RA 1, entidad 105 y a la CSR/Certificado 2
- URNs
  - Almacenamiento de histórico de estados
    - urn:mace:rediris.es:irisgrid:pki:csr:state:20050304142236:signed:10e190a0c7608fbe...2d425e6af7
- XML/LDIF
  - Ficheros de intercambio de información entre CA y RAs/Aux
- PHP (RAs), Perl (CA)
- PAPI (Control de acceso)

- pkirisgridRA
  - pkirisgridID
  - pkirisgridRaName
  - pkirisgridUsrCount
- pkirisgridUsr
  - pkirisgridID
  - cn
  - sn
  - telephoneNumber
  - mail

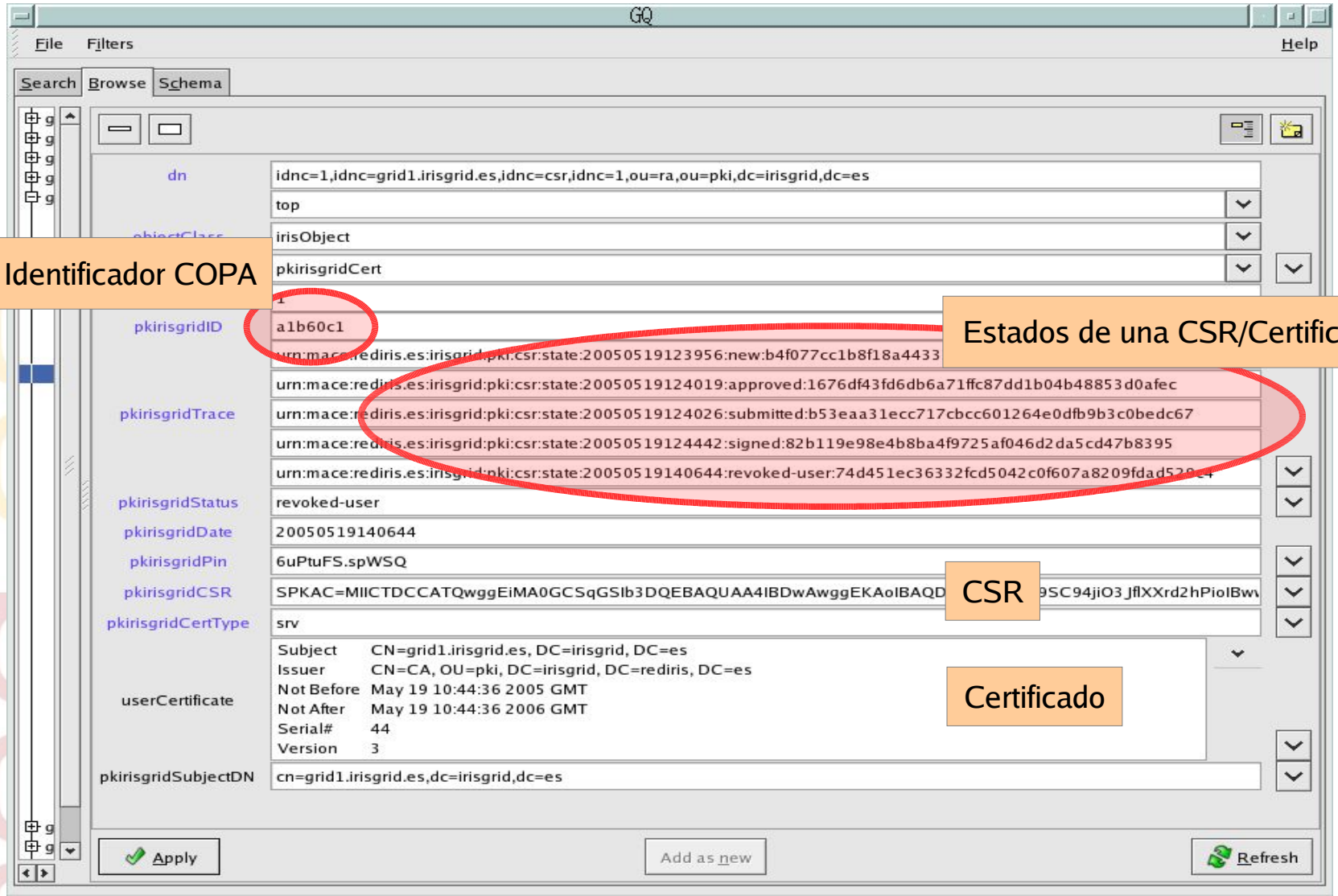
- pkirisgridCert
  - pkirisgridID
  - pkirisgridTrace
  - pkirisgridStatus
  - pkirisgridDate
  - pkirisgridPin
  - pkirisgridCSR
  - pkirisgridCertType
  - pkirisgridSubjectDN
  - userCertificate

a	Datos de las RAs
b	Datos de las entidades
c	Datos de los certificados



a2b105c2 identifica a la RA 2, entidad 105, y al certificado/CSR 2

pkIRISGrid v0.2 beta
Entrada de certificado almacenado en LDAP



Fichero XML con CSRs
enviadas a la CA para la generación de certificados

```
<pkig>
<csrs>
<csr>
  <csr_header>
    <type_nav>SPKAC</type_nav>
    <type_usr>usr</type_usr>
    <dn>idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es</dn>
    <serial>a2b2c1</serial>
    <trace>urn:mace:rediris.es:irisgrid:pki:csr:state:20050307171823:approved:2b4c41234ba13 ... bde675d</trace>
  </csr_header>
<csr_data>
CN = antonio.robles@org.es
1.DC = irisgrid
0.DC = es
SPKAC=MIICTDCCATQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDow69mjKY3R5/MPWuN0XW/GY
     0qF3iAUJCNZZ9Jlcz05+hpgp3g5K1E7KUE8eIW+T/eiSwC3KPH..... W+NHCr8rn/FOpoyGw==
</csr_data>
  <csr_sig>c01e06d357edce49ed301bd687dae35cb520e332</csr_sig>
</csr>

<csr>
      ...
</csr>
</csrs>
<total_sig>7a29946e2c0a649ca31d2f530122e2b39b2f3af9</total_sig>
</pkig>
```

Fichero LDIF con certificados
devueltos por la CA


```
# Fichero LDIF para volcar a la CA de la pkirisgrid
# Usuario: antonio.robles@org.es
dn: idnc=1,idnc=antonio.robles@org.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed
-
replace: pkirisgridDate
pkirisgridDate: 20050230131552
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:20050230131552:signed:86fc84c4778e38 ... 46fc52198adc
-
replace: userCertificate;binary
userCertificate;binary::MIIFGDCCBACgAwIBAgIBFjANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQDEwJAoGA1UE
 EAYKCZImiZPyLGQBGRMCZXMwHhcNMDUwMzMwMTExNTUxWhcNMDYwMzMwMTExNTUxWjBpMRIwEAYD
 ......
 K4Q3AKwSVVxlykqycV059KJN2MDJWlpur2+/FwjkUyrXJwUG5kLPyPu7Jnxd4k54ifpQKJB7NVXu
 HkM549/gD9zVlkY9jAKCzKpkkXgF4ghRcMvNAS7OCs/Z4N8MNzSsOVsArD3XNXGcG+0l7Kop
```

```
#Usuario:  towoto2.firefox@rediris.es
dn: idnc=1,idnc=towoto2.firefox@rediris.es,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: signed
.......
```

Fichero XML con CRRs
enviados a la CA

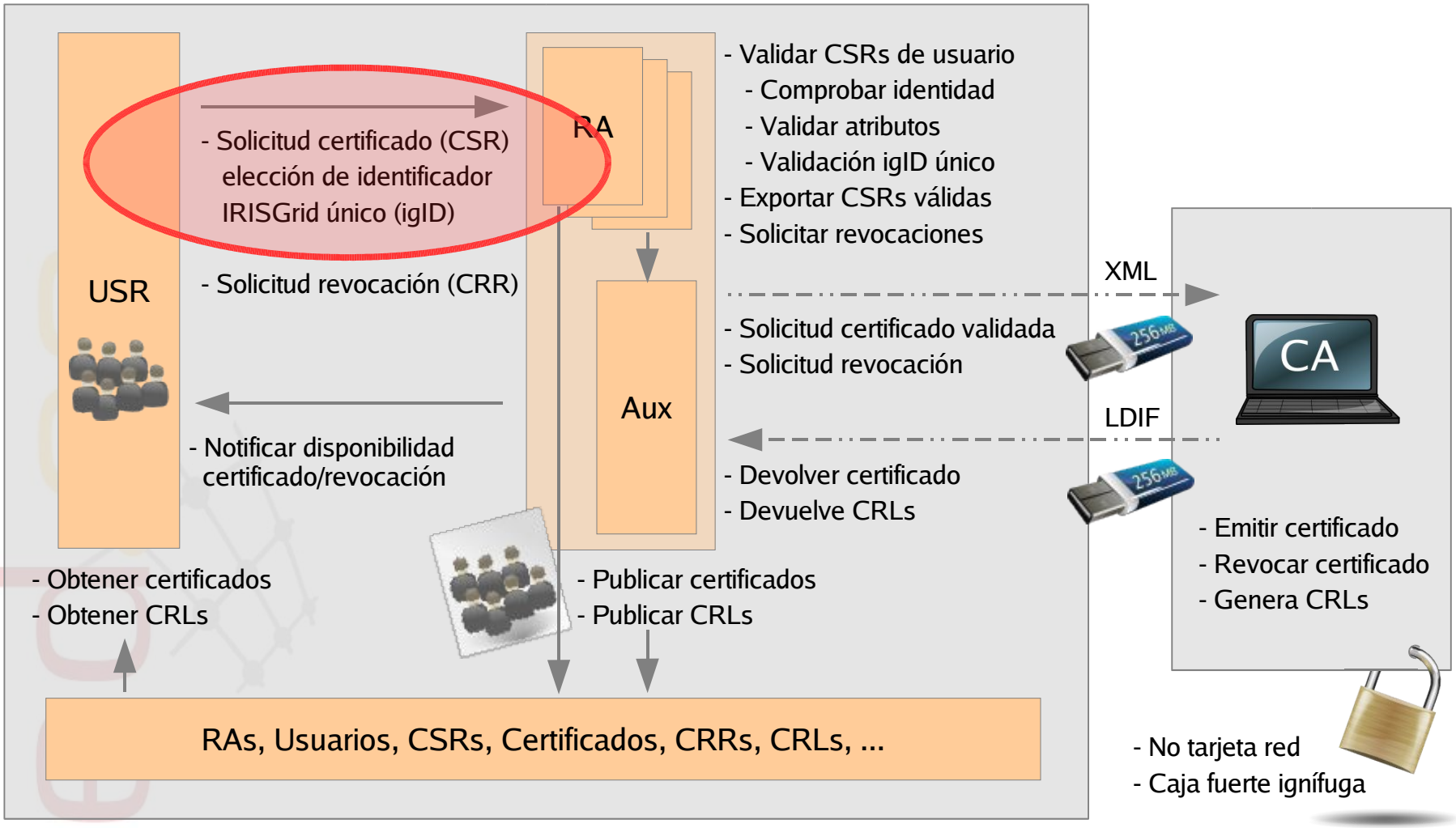
```
<pkig>
<crr_header>
  <crt_igID>a2b4c1</crt_igID>
  <crt_serial>22</crt_serial>
  <csr_dn>idnc=1,idnc=ww@ww.com,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es</csr_dn>
  <crr_ra>2</crr_ra>
  <crr_user>user</crr_user>
</crr_header>
<crr>
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 22 (0x16)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=CA, OU=pki, DC=irisgrid, DC=es
        Validity
            Not Before: Mar 30 11:15:51 2005 GMT
            Not After : Mar 30 11:15:51 2006 GMT
        Subject: CN=ww@ww.com, DC=irisgrid, DC=es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b8:ad:27:8e:03:95:b8:c6:18:0f:73:e2:df:b4:
                    6d:be:f5:2f:4c:b9:88:36:84:79:f5:93:6b:60:90:
....
-----END CERTIFICATE-----
</crr>
<sig>61479b34d197f5d2461da22dbf0b9c4112557a49</sig>
</pkig>
```

Fichero LDIF con revocaciones
devuelto por la CA

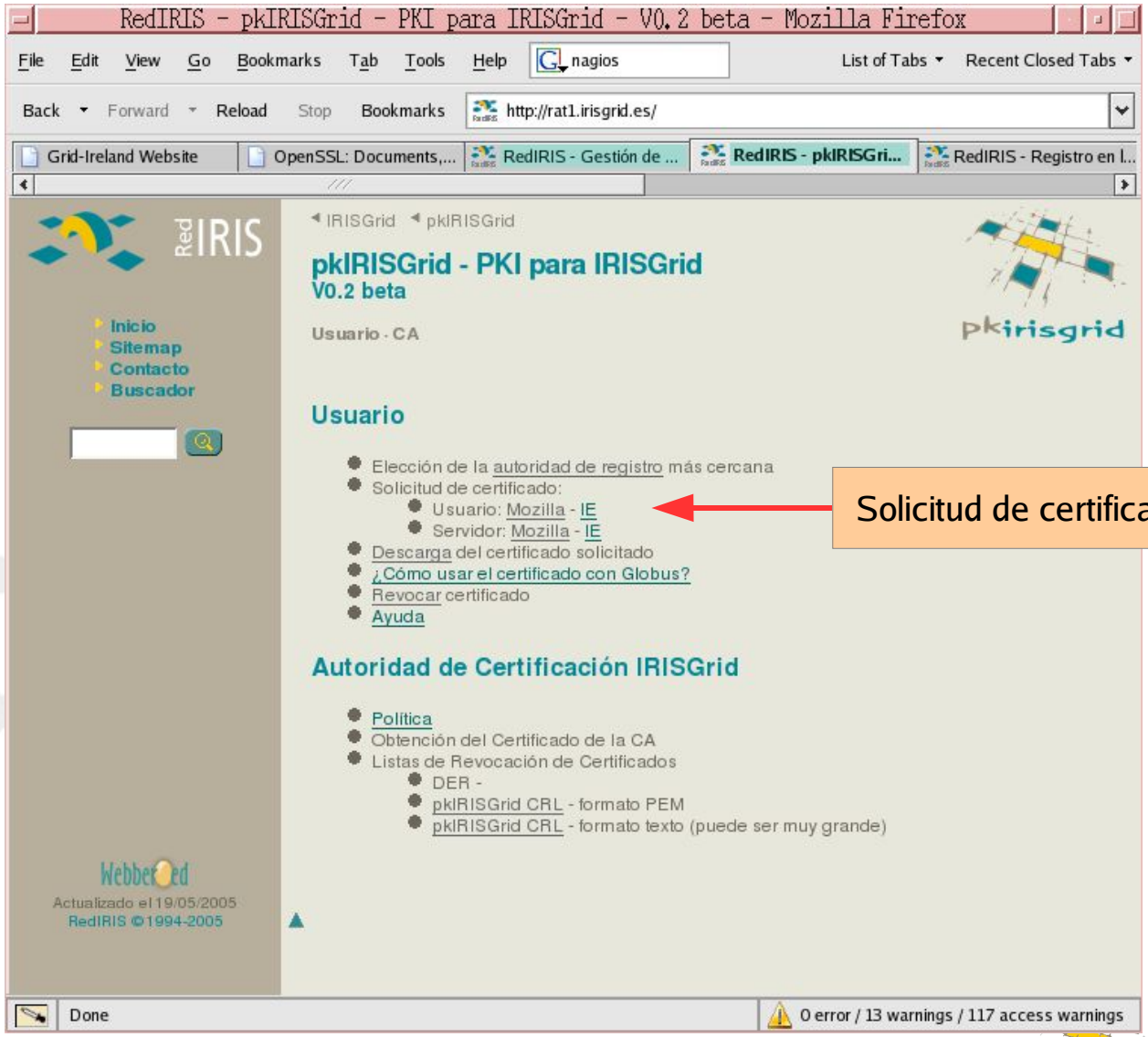
```
dn: idnc=1,idnc=ww@ww.com,idnc=csr,idnc=2,ou=ra,ou=pki,dc=irisgrid,dc=es
changetype: modify
replace: pkirisgridStatus
pkirisgridStatus: revoked-user
-
replace: pkirisgridDate
pkirisgridDate: 20050304142236
-
add: pkirisgridTrace
pkirisgridTrace: urn:mace:rediris.es:irisgrid:pki:csr:state:20050304142236:
    revoked-user:10e190a0c760 8fbe2d4...5f2ec57
```

- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- Tecnología usada
- Operación
  - Capturas de pantalla
- ¿Y ahora qué?

pkIRISGrid v0.2 beta
Solicitud de certificado

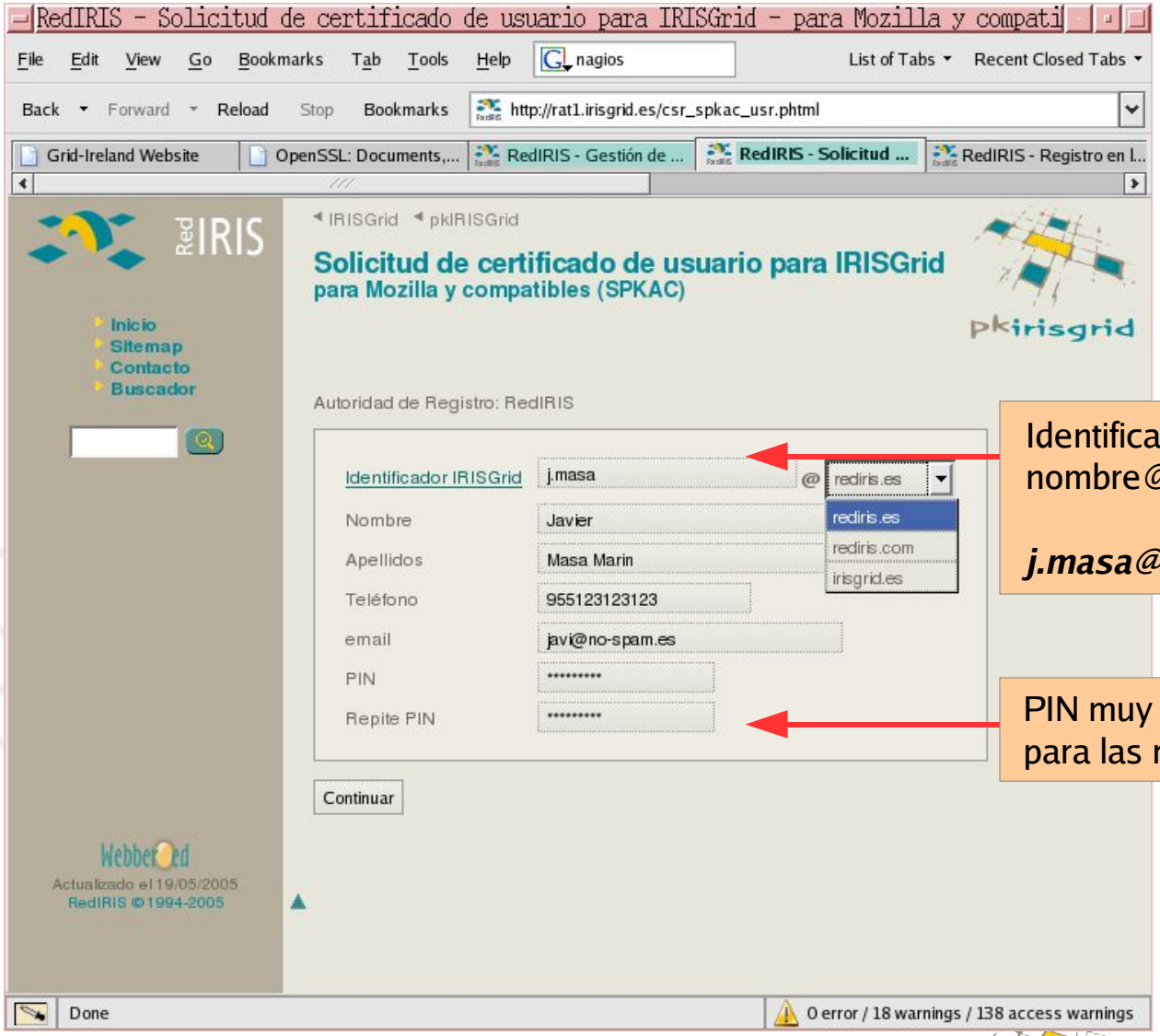


pkIRISGrid v0.2 beta
Solicitud de certificado con Mozilla



Solicitud de certificado con Mozilla

pkIRISGrid v0.2 beta
Formulario para la CSR

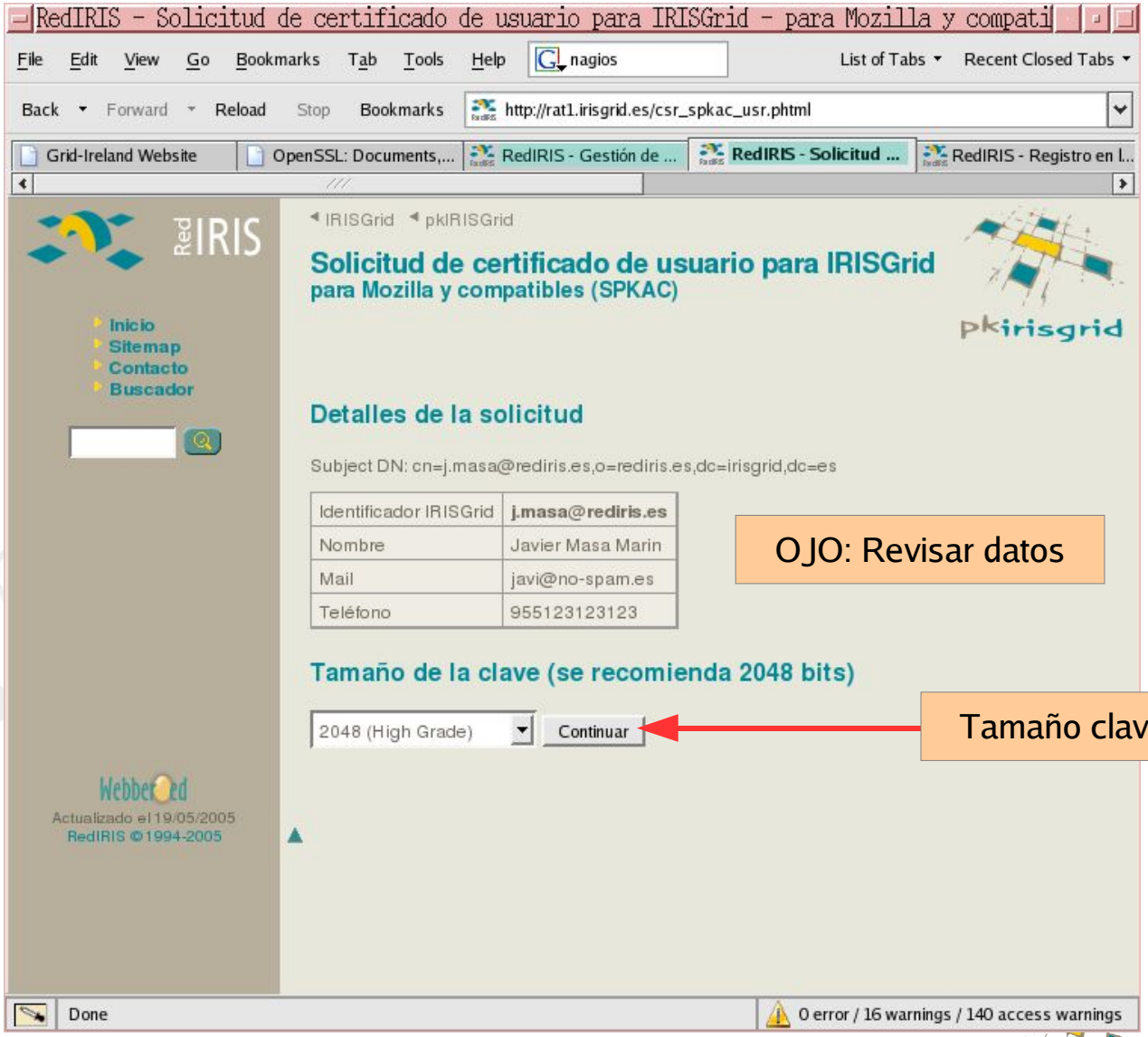


Identificador IRISGrid
nombre@org.dom

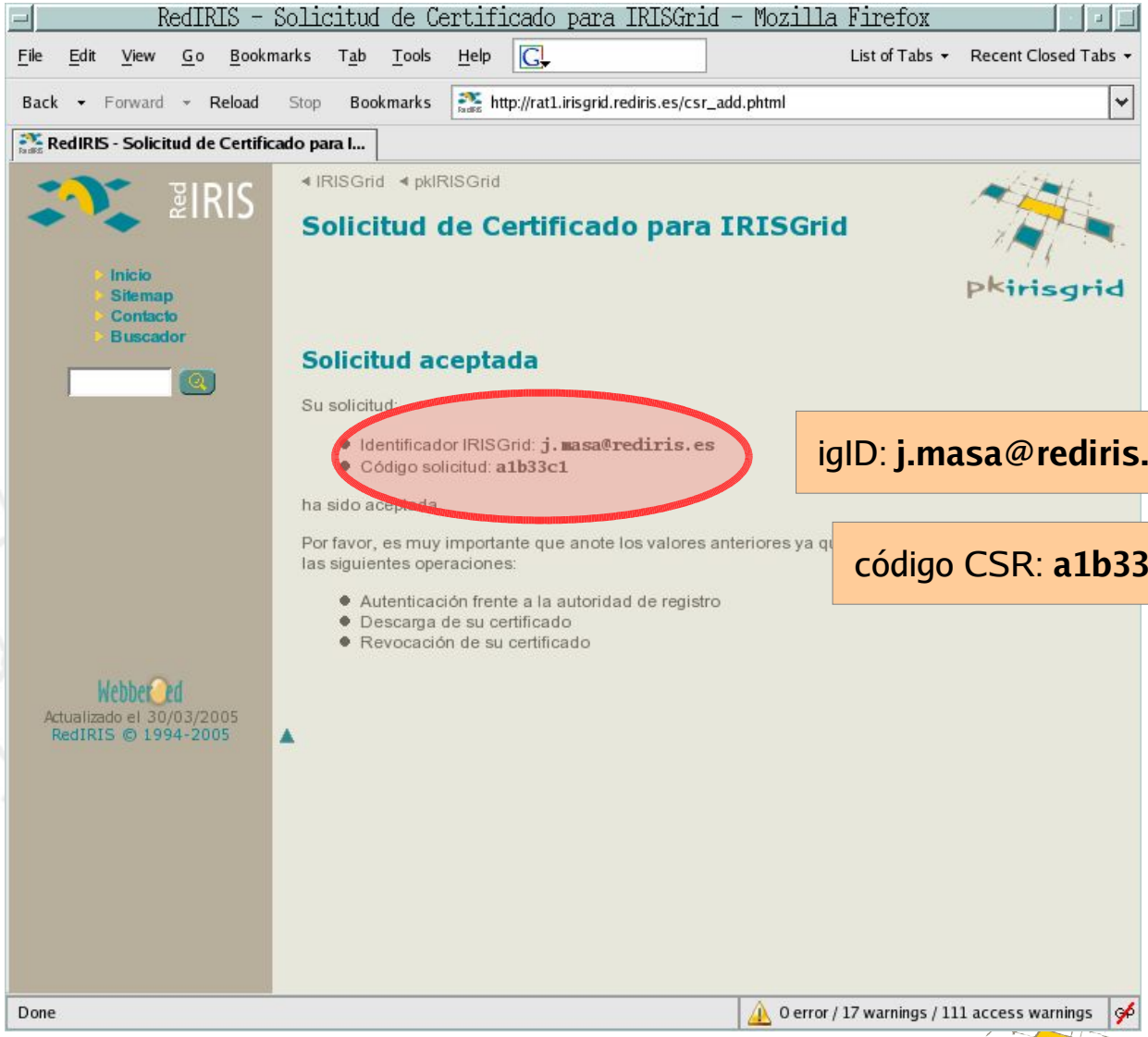
j.masa@rediris.es

PIN muy importante
para las revocaciones

pkIRISGrid v0.2 beta
Elección del tamaño de la clave para en la CSR



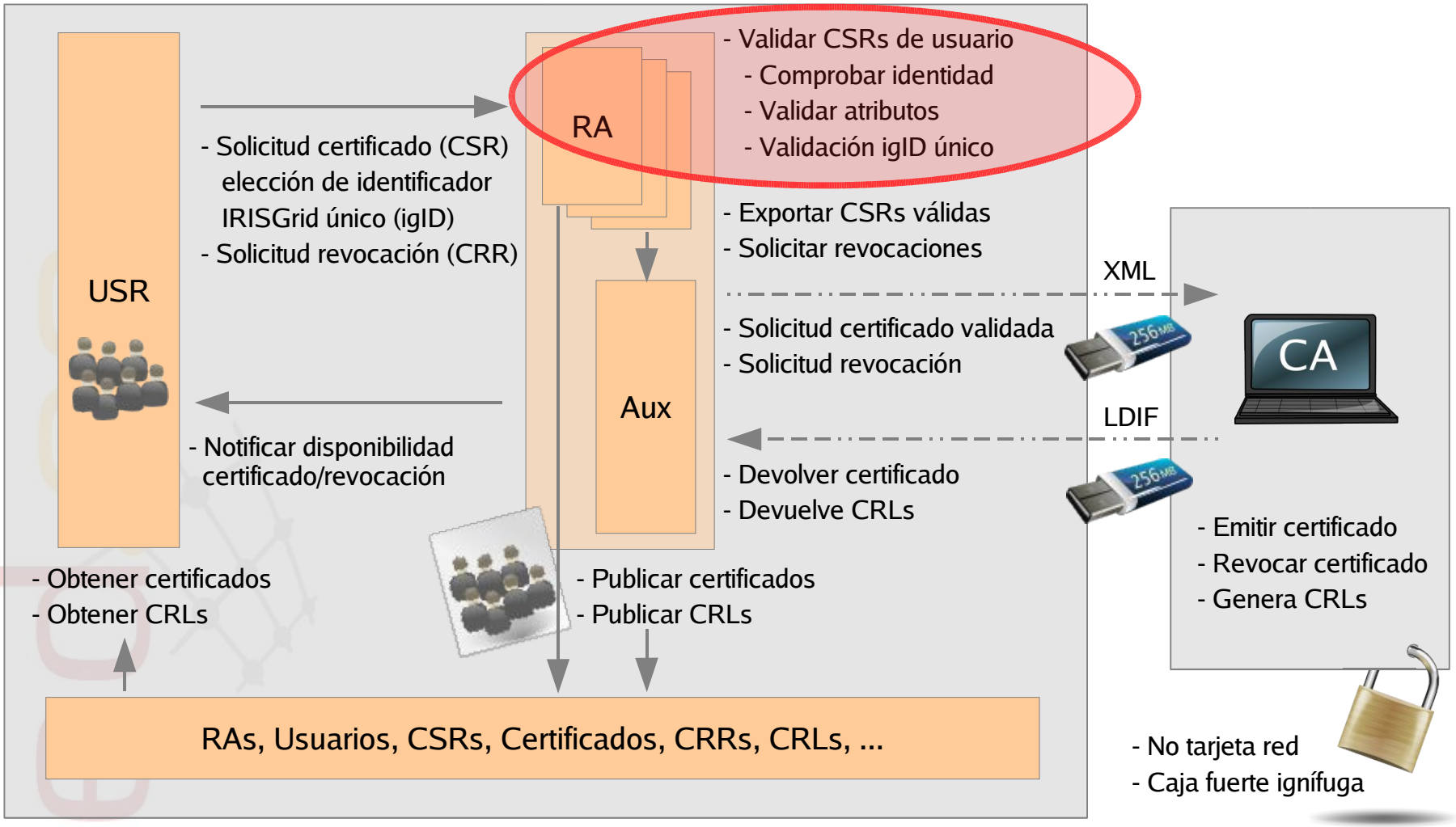
pkIRISGrid v0.2 beta
Solicitud de certificado aceptada



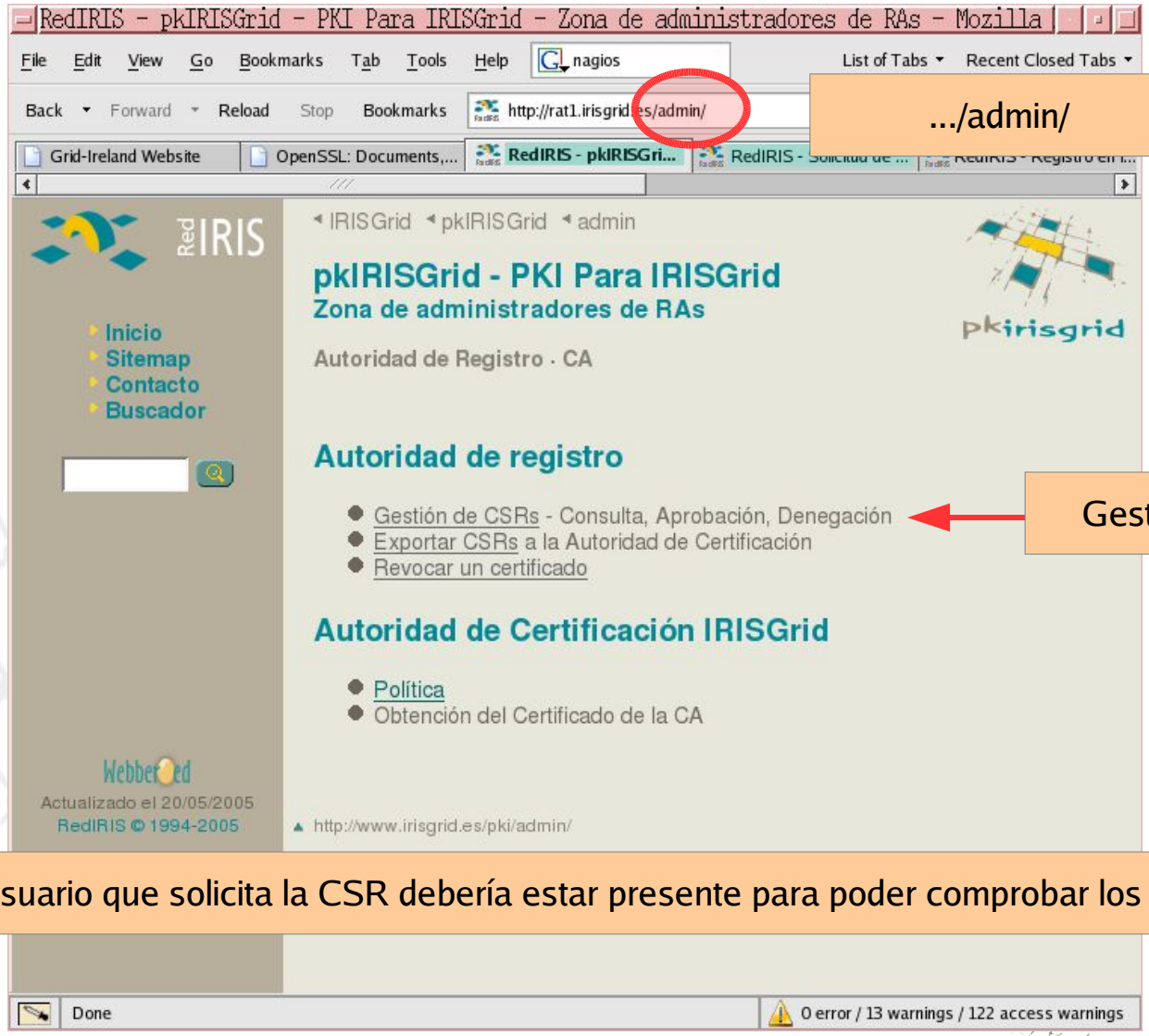
igID: **j.masa@rediris.es**

código CSR: **a1b33c1**

pkIRISGrid
Validación de usuario

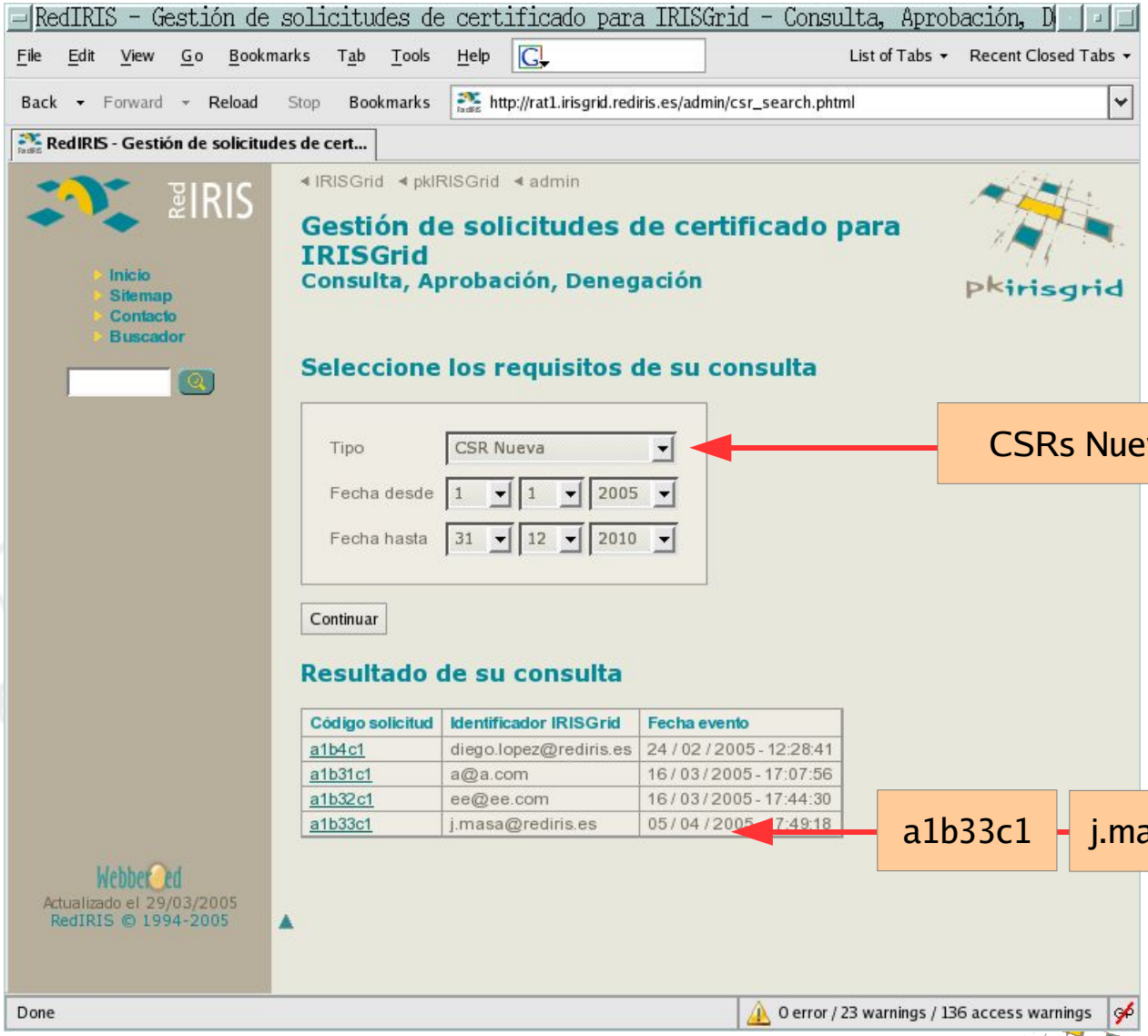


pkIRISGrid v0.2 beta
Gestión de CSRs



El usuario que solicita la CSR debería estar presente para poder comprobar los datos

pkIRISGrid v0.2 beta
Búsqueda de CSRs nuevas

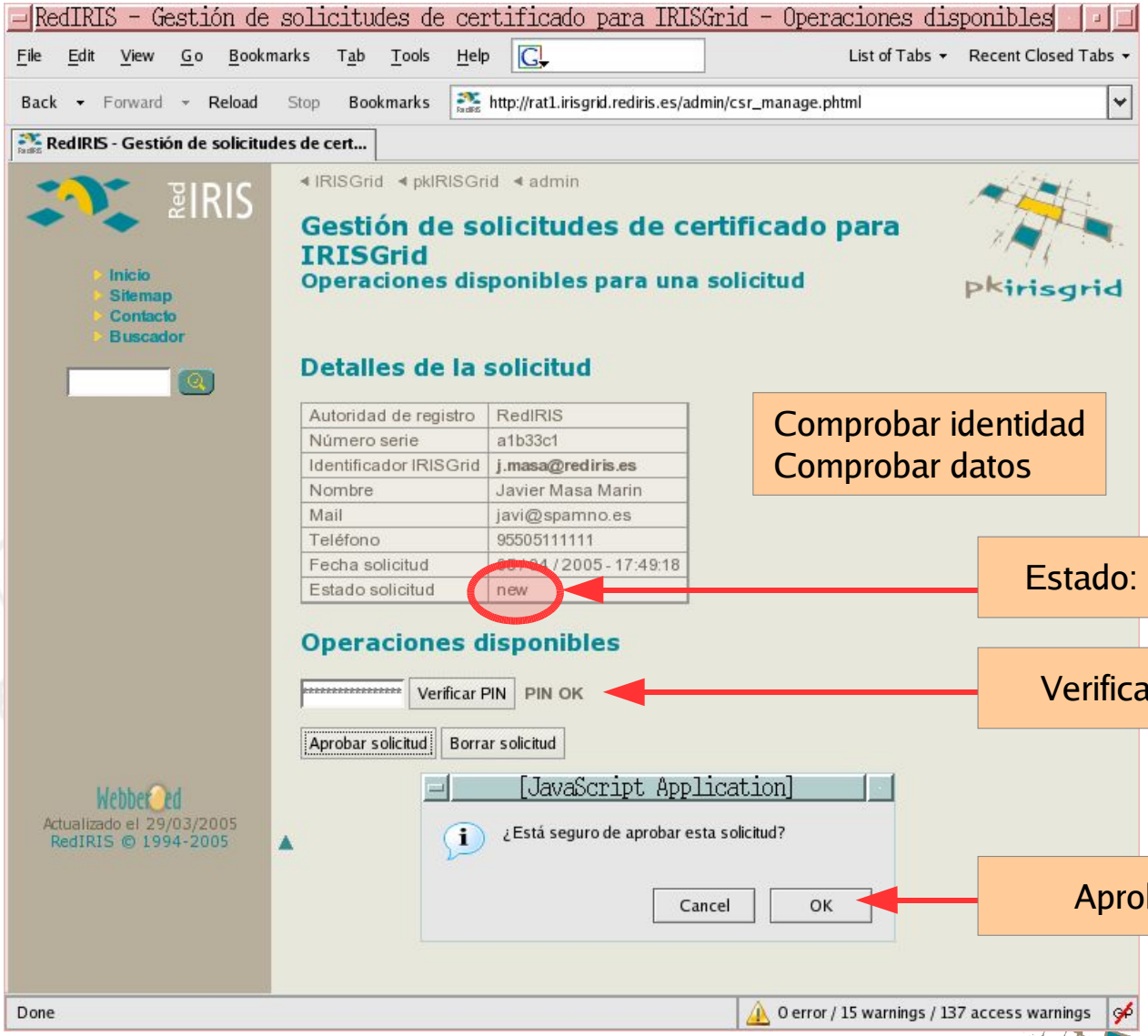


CSRs Nuevas

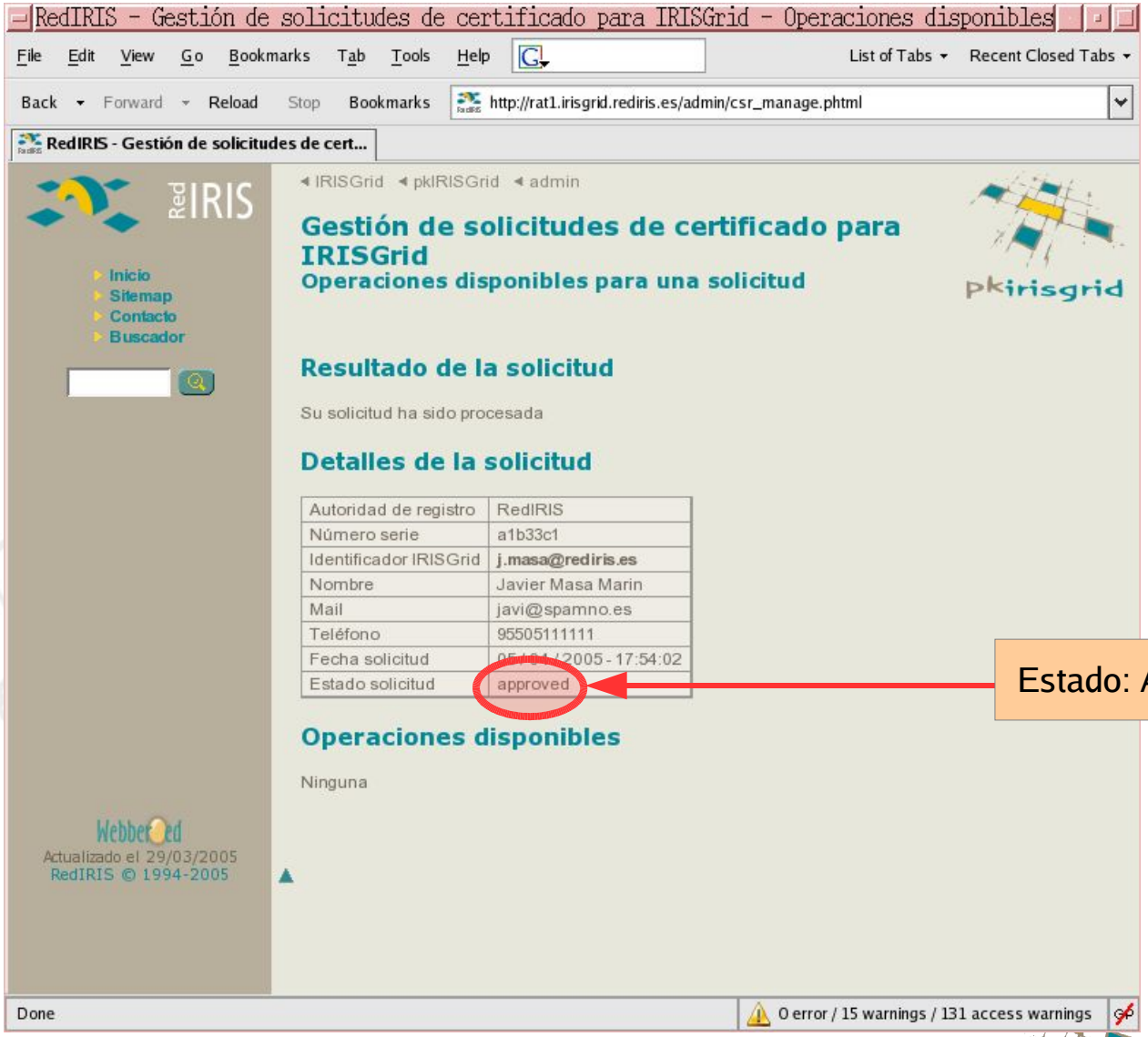
a1b33c1

j.masa@rediris.es

pkIRISGrid v0.2 beta
Aprobación de la CSR una vez validado el usuario

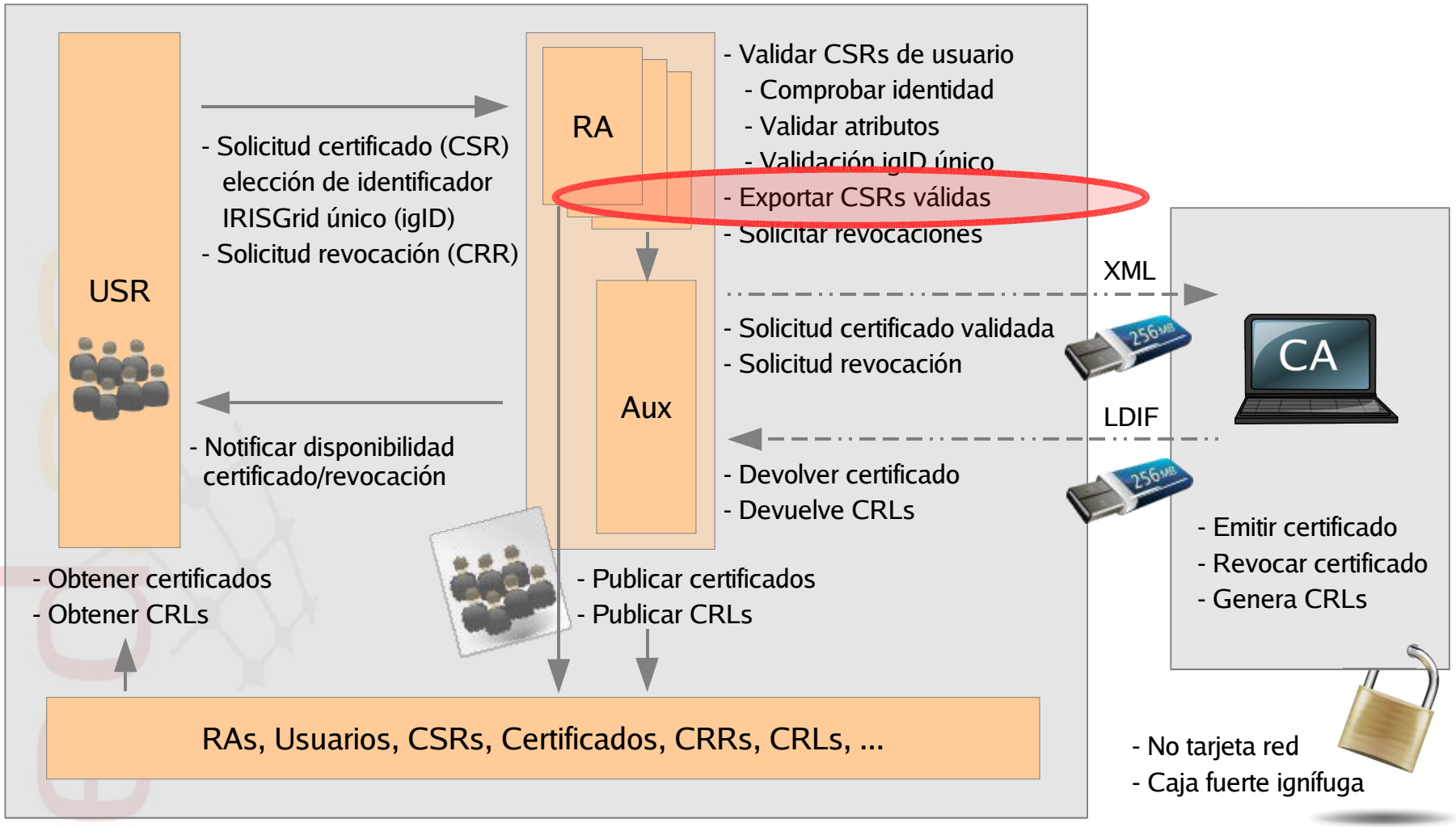


pkIRISGrid v0.2 beta
Resultado de la aprobación



Estado: Aprobada

pkIRISGrid
Exportación de las CSRs validadas por la RA

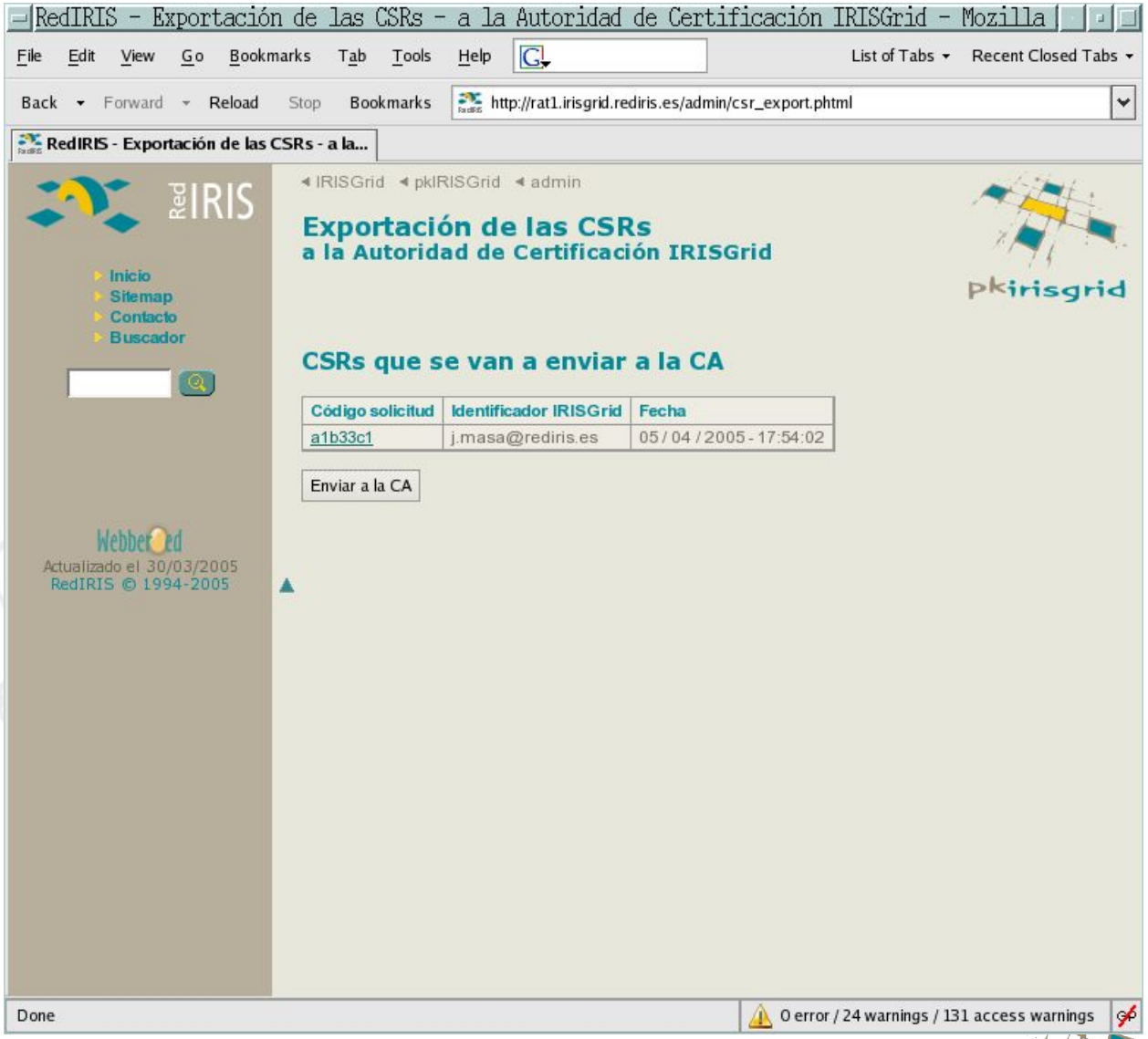


pkIRISGrid v0.2 beta
Exportar CSRs

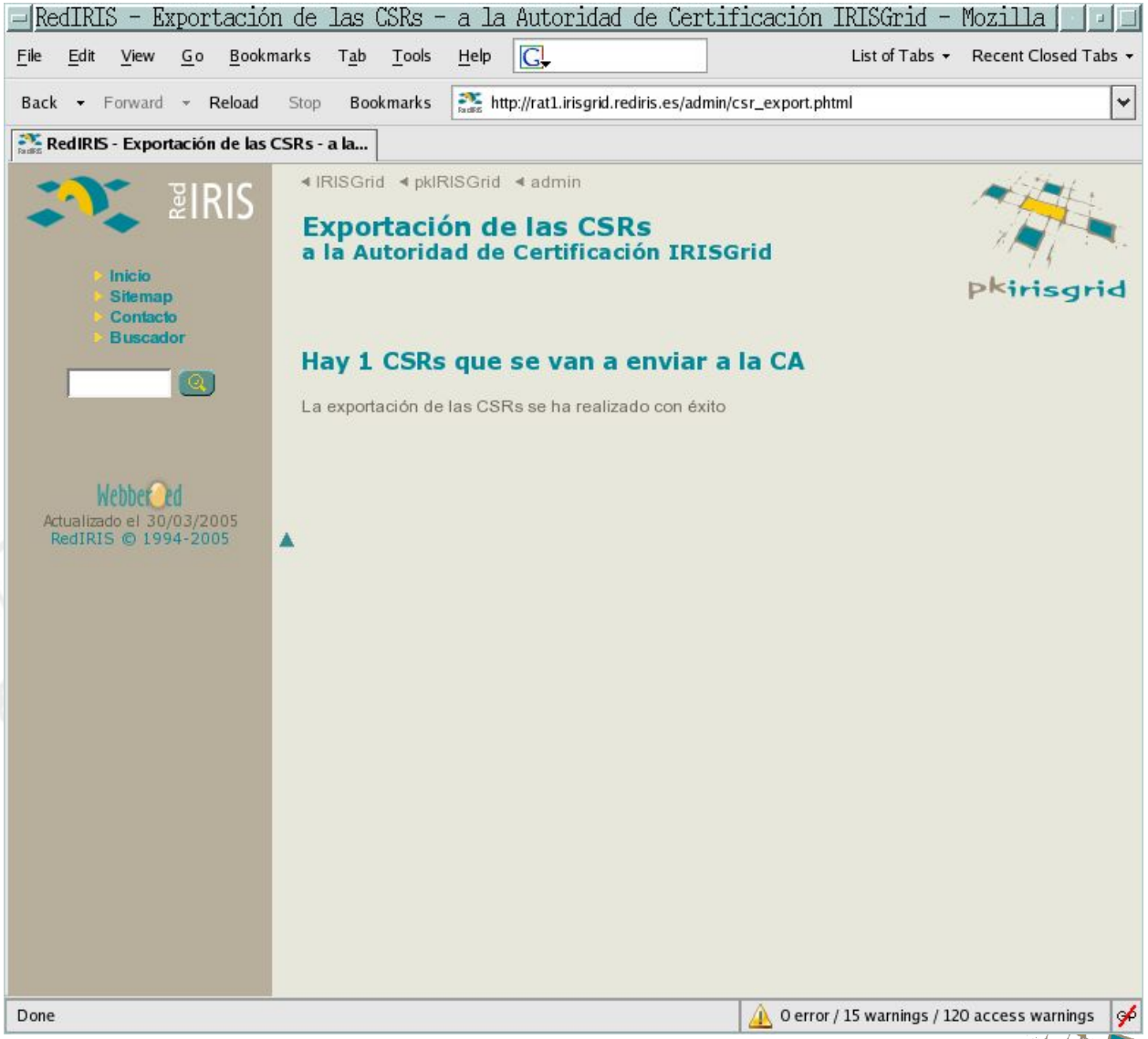
Exportar CSRs validadas

pkirisgrid

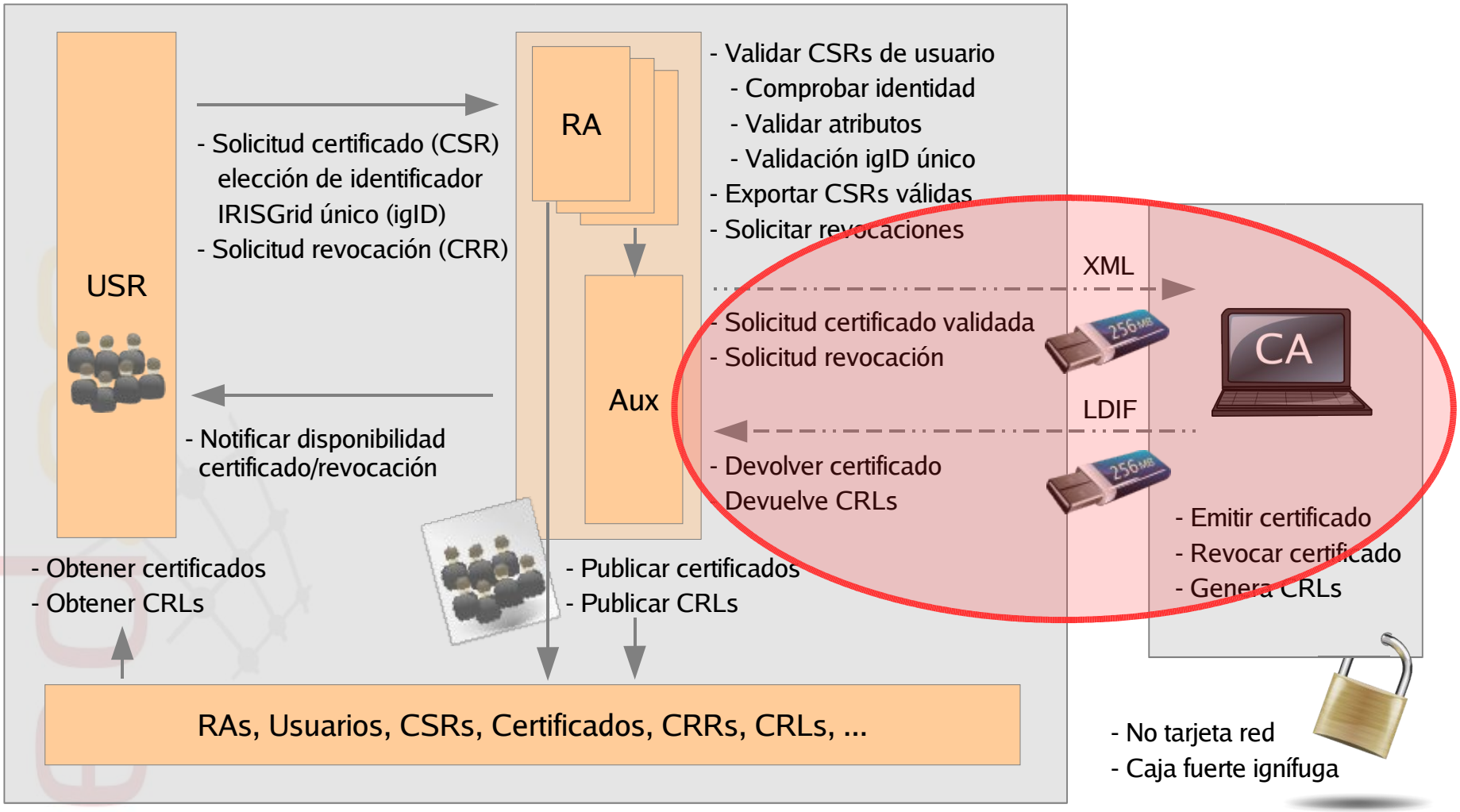
pkIRISGrid v0.2 beta
Listado de CSRs a exportar a la CA



pkIRISGrid v0.2 beta
Resultado de la exportación de CSRs

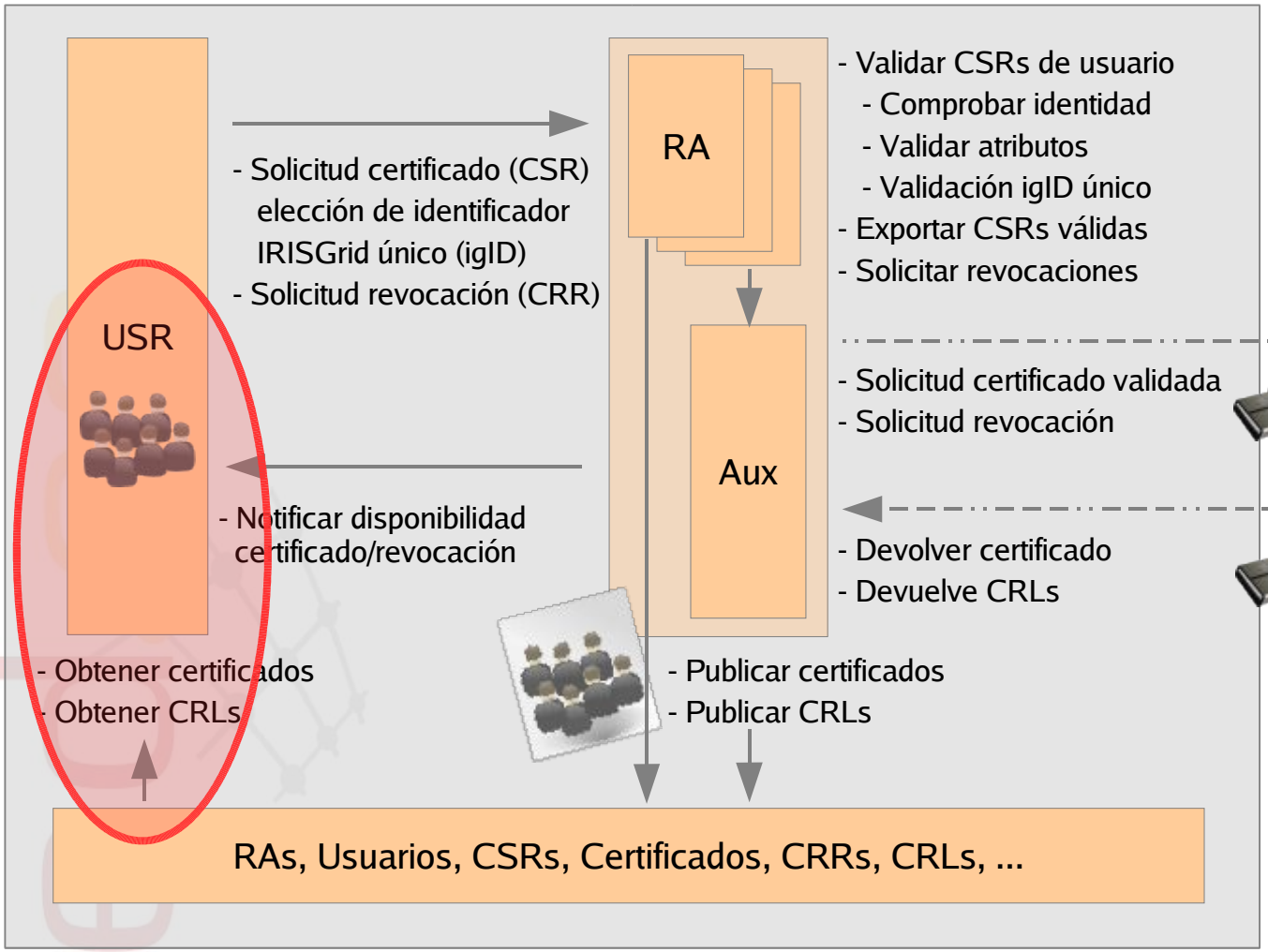


pkIRISGrid
Trabajo de la CA y módulo auxiliar de la RA

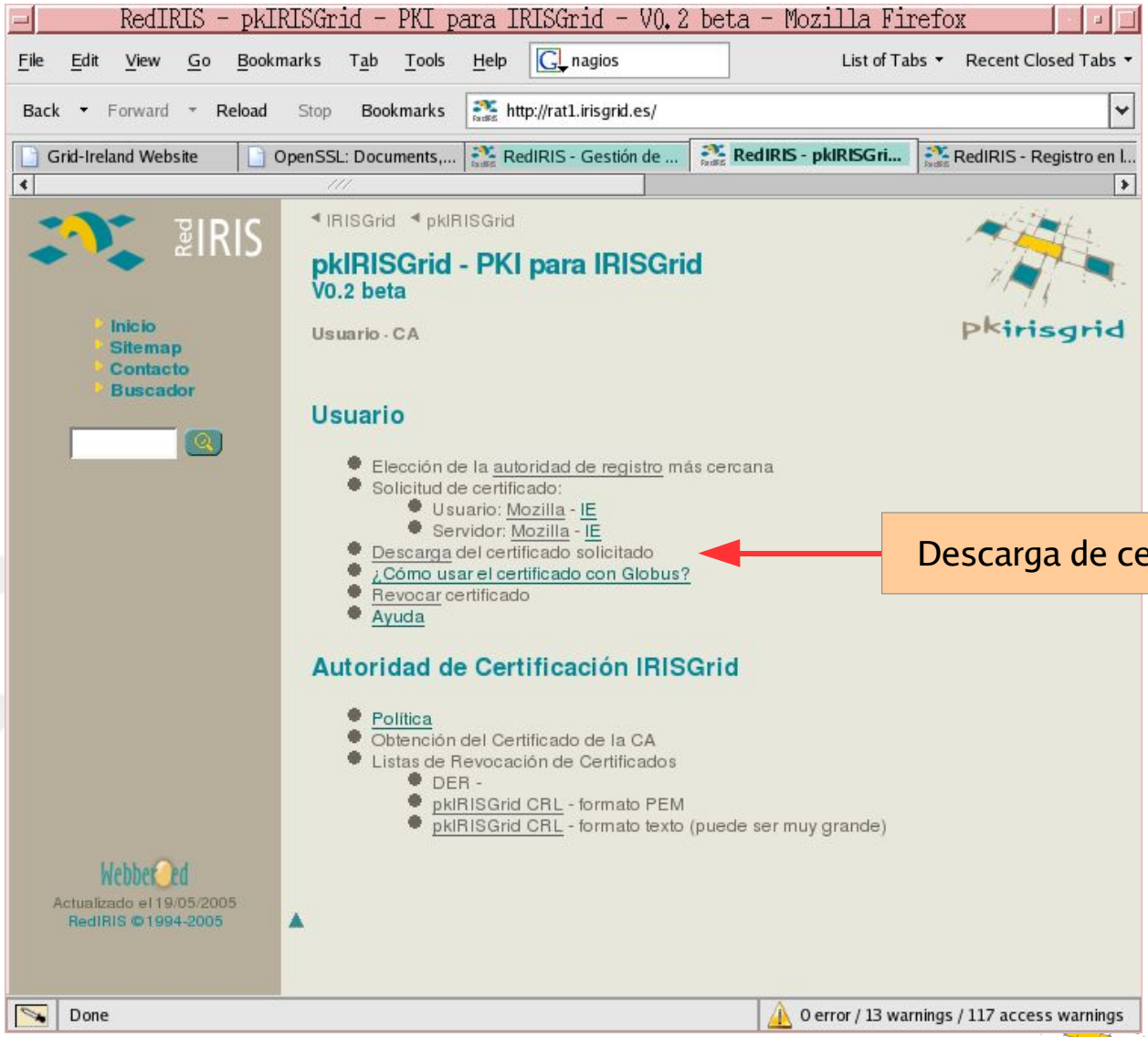


- Operador CA recibe las CSRs, CRRs
  - por mail, ftp, ... en formato XML
- Exporta esos ficheros XML a una llave USB
- Saca la CA del armario, la enciende y monta la llave USB
- Ejecuta el programa correspondiente (ca, crr, crl, ...)
  - Firma, Revoca, Genera CRL, ... y obtiene salidas LDIF
- Copia esos ficheros a la llave USB
- Desmonta la llave USB, apaga el PC **y lo guarda**
- Lleva la llave USB a un PC con acceso a la red
- Vuelca al LDAP todos los ficheros LDIF
  - Se actualizan los certificados, CRLs, trazas, ...

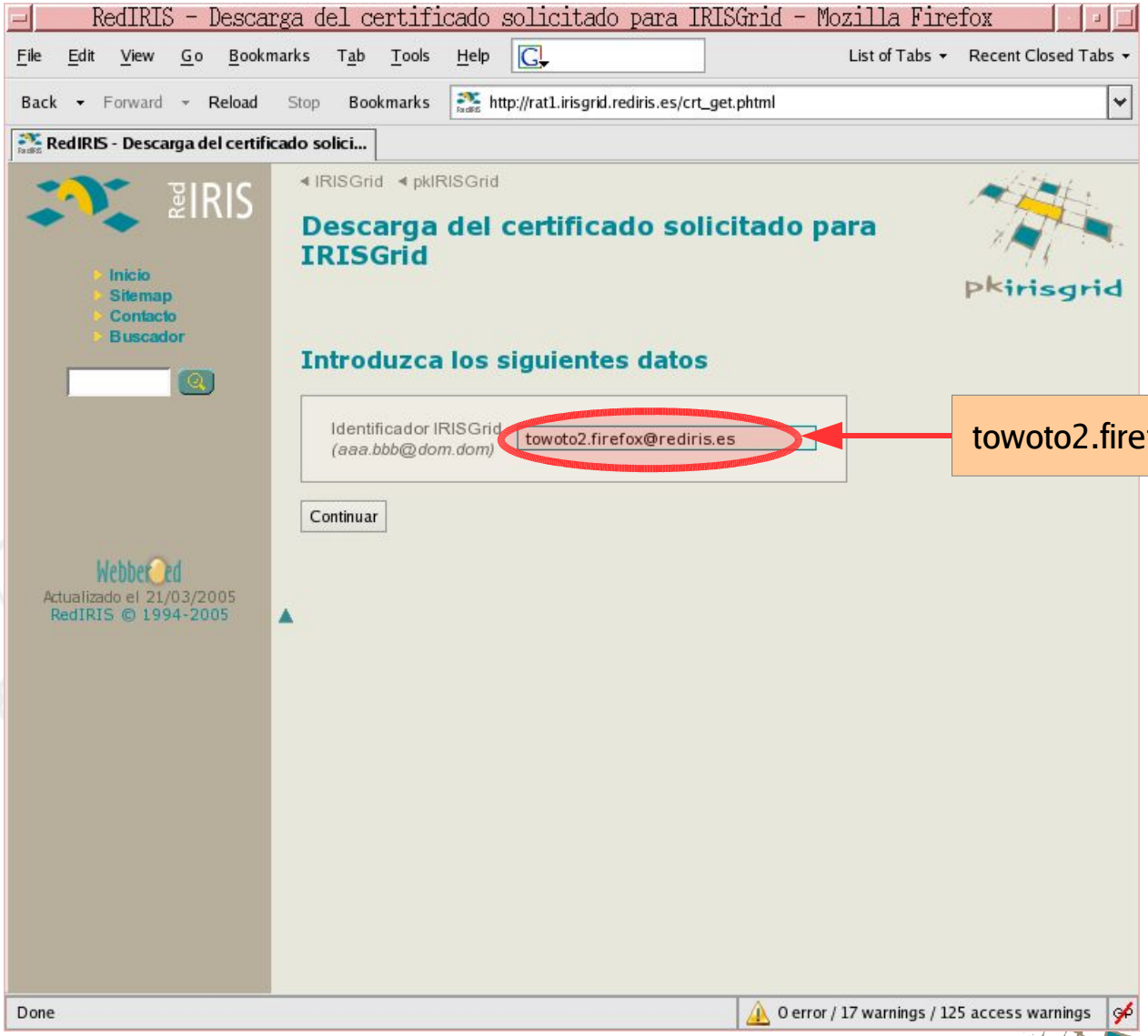
pkIRISGrid
Obtención del certificado por el usuario



pkIRISGrid v0.2 beta
Descarga del certificado

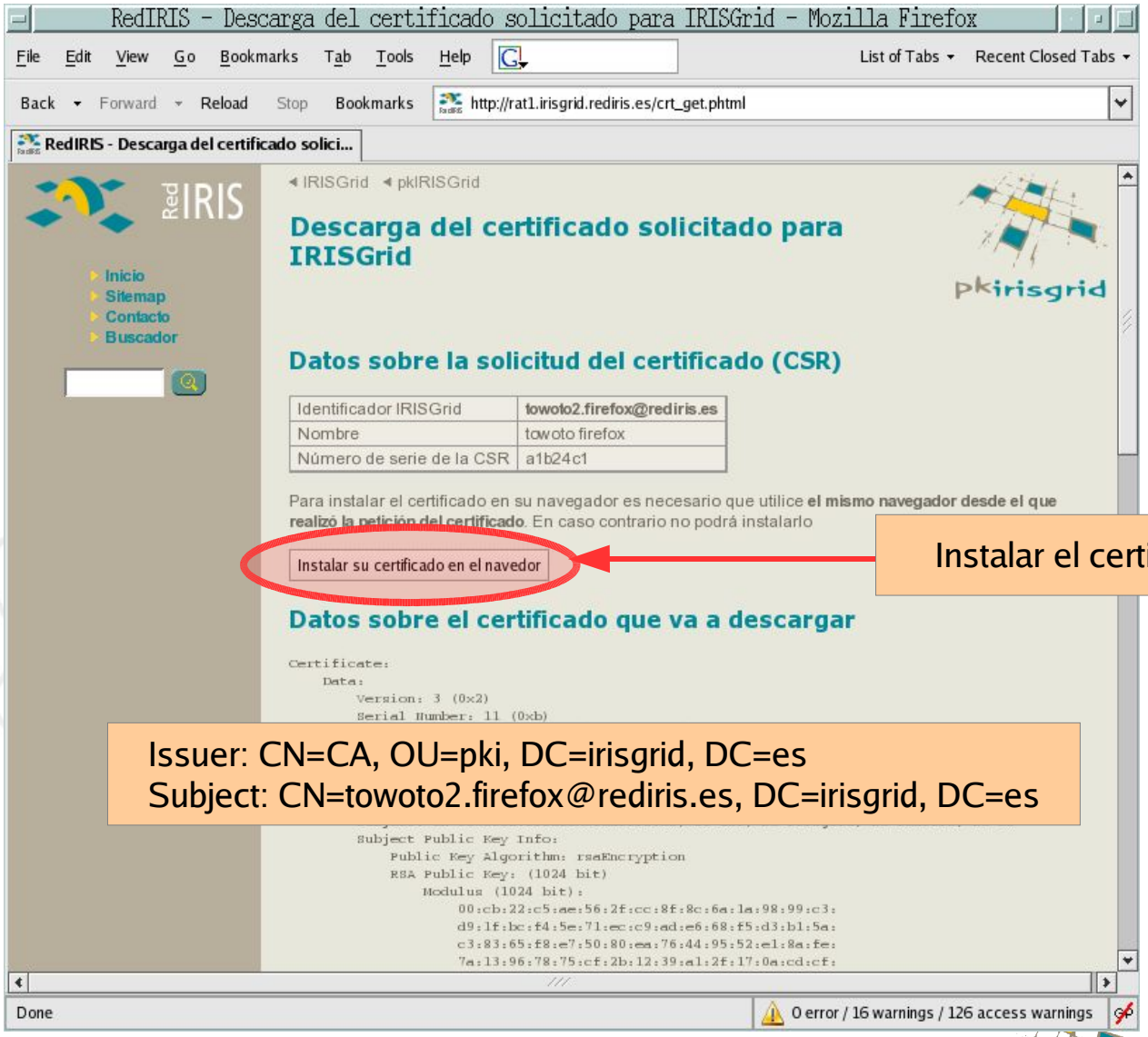


pkIRISGrid v0.2 beta
Selección del certificado



towoto2.firefox@rediris.es

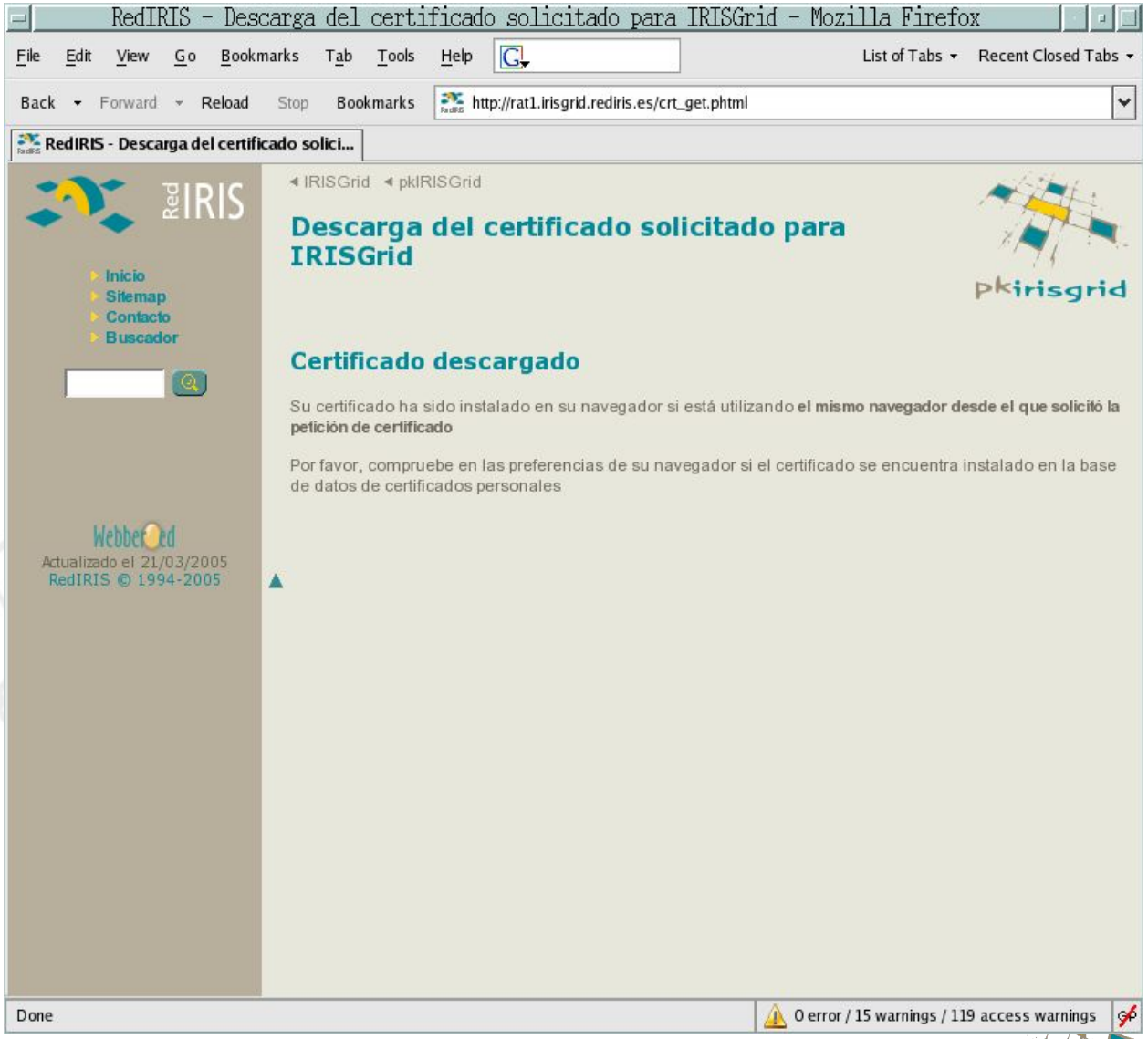
pkIRISGrid v0.2 beta
Comprobación de datos del certificado



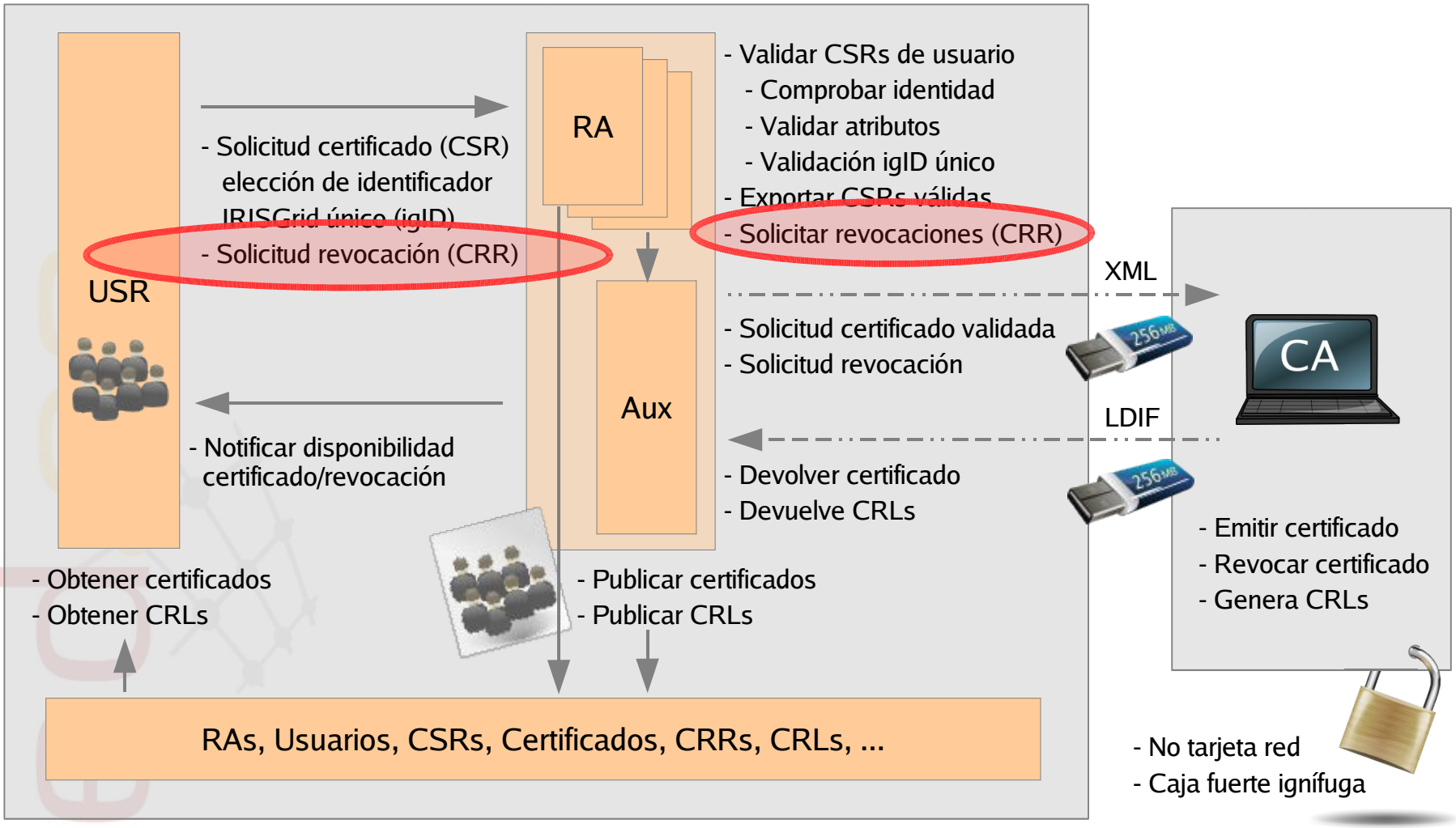
Instalar el certificado

Issuer: CN=CA, OU=pki, DC=irisgrid, DC=es
Subject: CN=towoto2.firefox@rediris.es, DC=irisgrid, DC=es

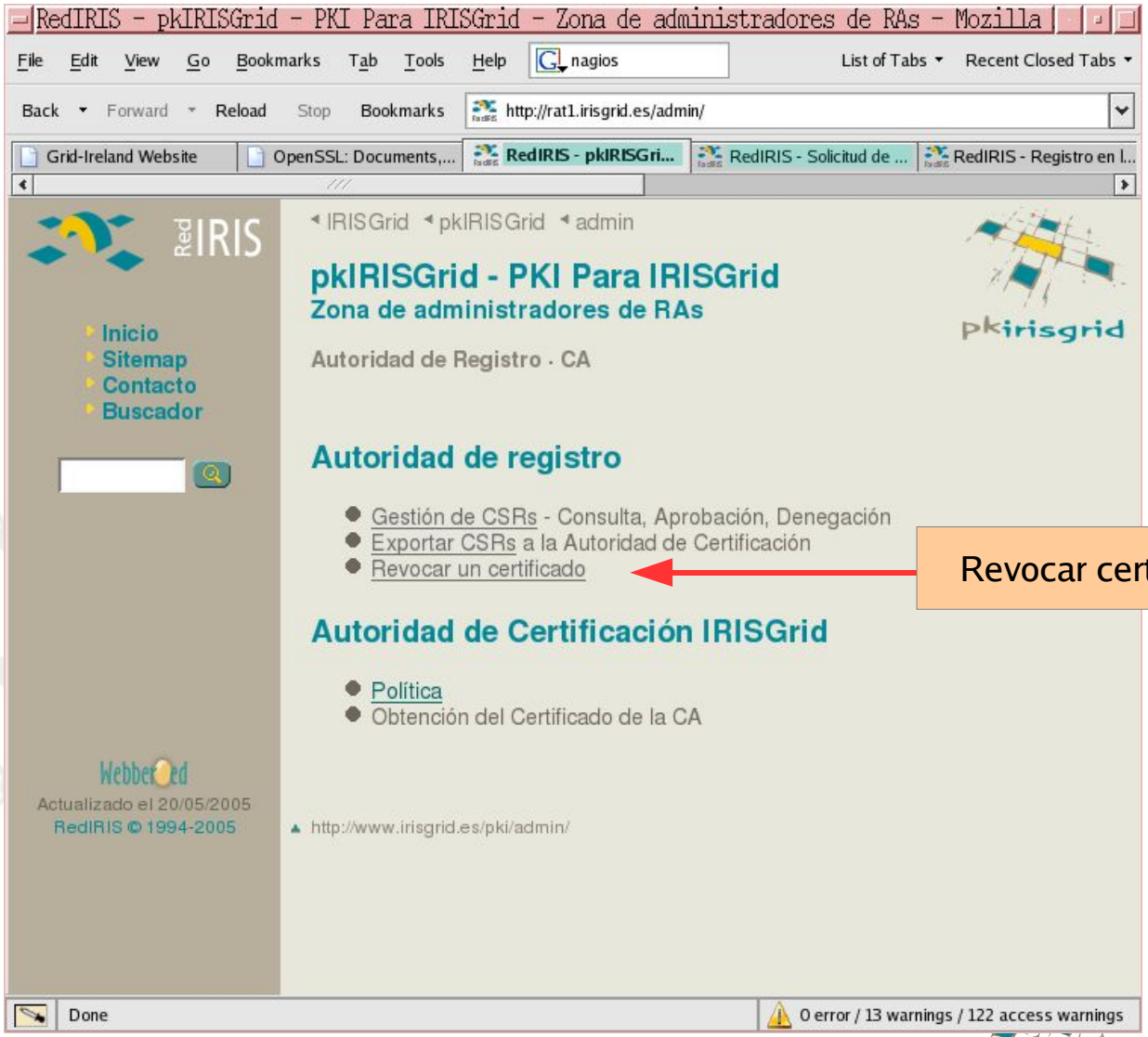
pkIRISGrid v0.2 beta
Instalación del certificado en el navegador



pkIRISGrid
Solicitud de revocación de certificado



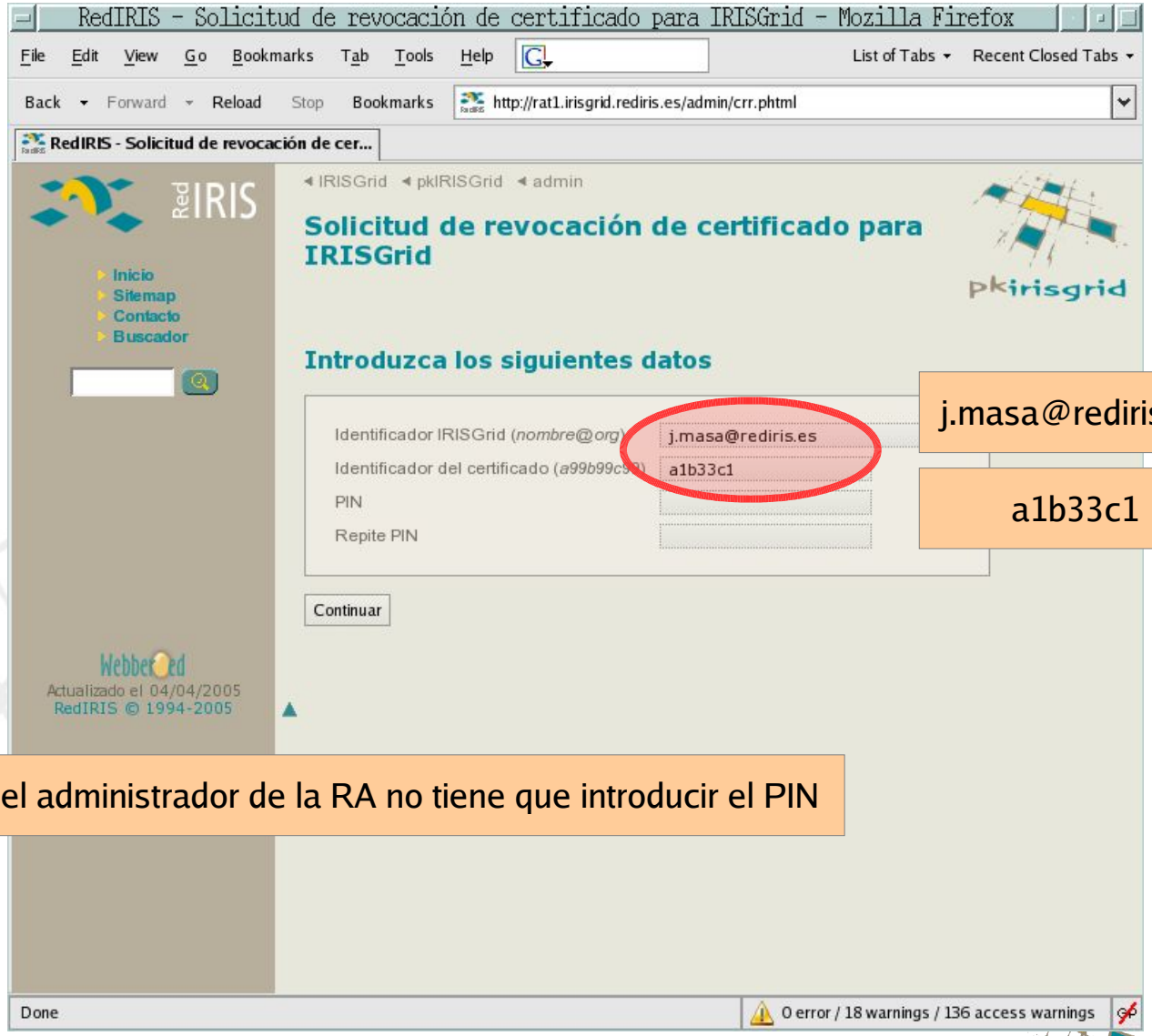
pkIRISGrid v0.2 beta
Revocación de certificado por administrador de RA



Revocar certificado

pkirisgrid

pkIRISGrid v0.2 beta
Introducción de datos del certificado a revocar

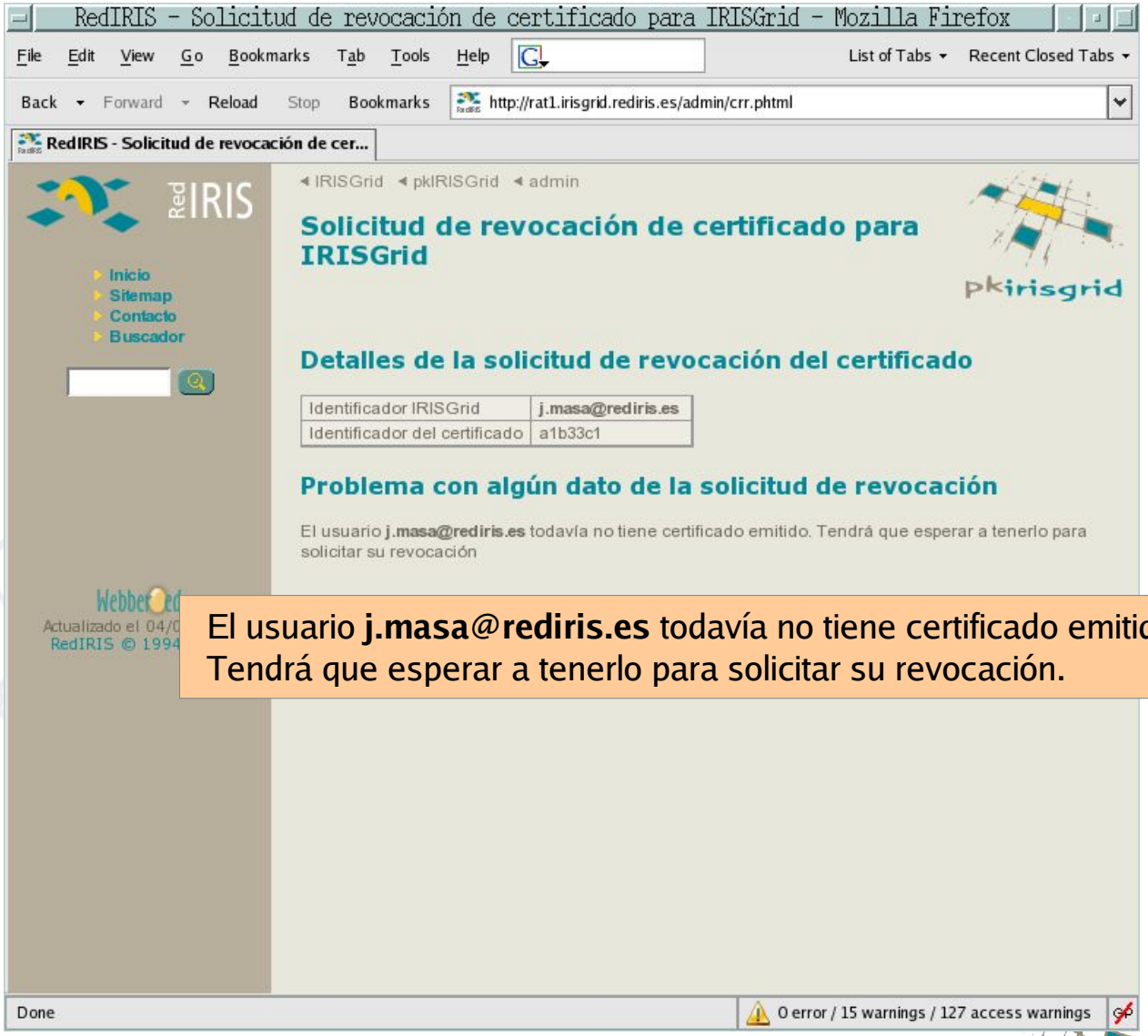


j.masa@rediris.es

a1b33c1

Si es el administrador de la RA no tiene que introducir el PIN

PkIRISGrid v0.2 beta
Problema al revocar un certificado inexistente



El usuario **j.masa@rediris.es** todavía no tiene certificado emitido. Tendrá que esperar a tenerlo para solicitar su revocación.

PkIRISGrid 0.2beta

- Requisitos pkIRISGrid 0.2 beta - EUGridPMA
- Estructura
- Tecnología usada
- Operación
  - Capturas de pantalla
- ¿Y ahora qué?

¿Y ahora qué?

- Política
  - Vamos a desarrollar las políticas
- Proceso de acreditación EUGridPMA
- Beta de pkIRISGrid
  - Uso de la actual identidad de la CA de IRISGrid
  - Creación de varias RAs
  - Los certificados que sigan siendo válidos al finalizar la beta se refirmarán con la identidad definitiva de la CA
- Ampliación de pkIRISGrid
  - Vuestras sugerencias

- RA de ejemplo
  - http://rat1.irisgrid.es
  - http://rat1.irisgrid.es/admin/
- Esquema LDAP pkirisgrid
  - http://www.rediris.es/ldap/esquemas/
- Esta presentación **estará** disponible en
  - http://www.irisgrid.es/coord/gt/gt2005/gt2005-pkirisgrid.pdf
- Mail
  - javier.masa@rediris.es